COMODO BR

Criando Confiança da Web

TUTORIAIS E PROCEDIMENTOS

Exportando do IIS para Apache

Criar um snap-in do MMC para gerenciar certificados

Para fazer o backup, primeiro crie um novo MMC e adicione o snap-in de certificados.

Use o procedimento a seguir para criar um novo MMC e adicionar o snap-in de certificados:

1. Clique em Iniciar e em Executar.
2. Digite "MMC.EXE" (sem as aspas) e clique em OK.
3. Clique em Console no novo MMC criado e, em seguida, clique em Adicionar/remover snap-in.
4. Na nova janela exibida, clique em Adicionar.
5. Selecione Certificados e clique em Adicionar.
6. Escolha a opção Conta de computador e clique em Avançar.
7. Selecione Computador local na próxima tela e clique em OK.
8. Clique em Fechar e, em seguida, em OK.

Agora, você adicionou o snap-in de certificados, que lhe permitirá trabalhar com quaisquer certificados no armazenamento de certificado do seu computador.

Exportar uma chave pública e uma chave privada

Agora que já adicionou o snap-in de certificados, você poderá exportar o par de chaves que seu servidor Web está usando (a chave pública e a chave privada). Para fazer isso, execute as seguintes etapas:

1. Abra o snap-in de certificados (Computador local) que você adicionou na última seção, navegue até Pessoal e, depois, até Certificados.
2. O certificado do seu servidor Web estará indicado pelo CN (Common Name) encontrado no campo Assunto do certificado (usando o Internet Explorer 5.0, você poderá exibir facilmente o certificado para ver o Common Name, caso não saiba qual é ele).
3. Clique com o botão direito do mouse no certificado do servidor, selecione Todas as tarefas e clique em Exportar.
4. Quando o assistente for iniciado, clique em Avançar. Escolha exportar a chave particular e clique em Avançar.
5. Selecione o formato de arquivo “PKCS #12” (.PFX).

OBS: ao exportar o certificado para uso em um servidor Web com o Apache, não selecione “Exigir criptografia de dados de alta segurança”.

OBS: não selecione “Incluir todos os certificados no caminho de certificação, se possível”. Os certificados das autoridades emissoras podem ser exportados separadamente ou solicitados ao departamento de Suporte.

6. Clique em Avançar e escolha uma senha para proteger o arquivo PFX. Será necessário inserir a mesma senha duas vezes para garantir que ela foi digitada corretamente. Ao concluir essa etapa, clique em Avançar.
7. Escolha o nome com o qual deseja salvar esse arquivo. Não inclua uma extensão no nome do arquivo; o assistente adicionará automaticamente a extensão PFX para você.
8. Clique em Avançar e leia o resumo. Preste atenção especial ao local em que o arquivo está sendo salvo. Se tiver certeza de que as informações estão corretas, escolha Concluir.

Agora, você tem um arquivo PFX que contém o certificado do seu servidor e a respectiva chave privada correspondente.

Converter o arquivo .PFX para uso com o Apache

Para converter o arquivo e extrair a chave privada você deve usar o aplicativo OpenSSL em uma linha de console, com o comando:

```
openssl pkcs12 -in [nome do arquivo.pfx] -out [nome do novo arquivo.txt]
```

Quando solicitado, entre com a mesma senha usada ao exportar o certificado.

Abra o arquivo .txt gerado em um editor de textos e salve cada seção em um arquivo separado. Para a chave privada normalmente é usada a extensão .key, para o certificado, .cer.

As seções são delimitadas por linhas semelhantes a

`-----BEGIN RSA PRIVATE KEY-----` e `-----END RSA PRIVATE KEY-----` **(chave privada)**

`-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` **(o seu certificado)**

Os arquivos devem ser configurados no Apache no respectivo httpd.conf, junto com os arquivos das autoridades certificadoras correspondentes.

Se o Apache não suportar o uso de chaves privadas criptografadas, use o comando a seguir para decriptografá-la:

```
openssl rsa -in [nome do arquivo da chave privada .key] -out [nova chave .key]
```